Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

-- 1. (currently amended) A method for communicating between a sender and a receiver over a computer network, comprising the steps of:

defining a plurality of parameters for a secure message, at least one of the plurality of parameters accessible to a management module for controlling receiver access to a decryption key;

sending the secure message from the sender to the receiver over a network;

receiving the secure message at the receiver;

sending a request from the receiver to a management module for the decryption key;

processing the request at the management module to determine whether the receiver is permitted to decrypt the message based on said at least one of the plurality of parameters;

when not permitted, sending a denial message to the receiver;

when permitted, sending the decryption key to the receiver; and

when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, ~~and~~ deleting the decryption key and preventing access to the decrypted message in the source format after said reformatting by deleting the source-formatted decrypted message.

2. (original) The method of claim 1, wherein the step of defining comprises the steps of:

sending a key length parameter from the sender to the management module;

deriving at the management module a key having a length corresponding to the key length parameter; and

defining a message code parameter to correspond to and be sent with the secure message; and

wherein the step of sending a request comprises sending a request including the message code to the management module.

3. (original) The method of claim 1, wherein the step of defining comprises the steps of:

sending a key parameter from the sender to the management module;

storing the key parameter at the management module as the decryption key;

defining a message code parameter to correspond to and be sent with the secure message, the message code being stored at the sender and at the management module; and

wherein the step of sending a request comprises sending a request including the message code from the receiver to the management module.

4. (original) The method of claim 1, wherein the step of defining comprises the steps of defining a message identification code and defining an access parameter used for determining receiver access to the decryption key of the secure message which corresponds to the message code, said access parameter being accessible to the management module, wherein the step of sending a request comprises sending the message code from the receiver to the management module, and wherein the step of processing the

request comprises testing the access parameter corresponding to the message code to determine whether the receiver is permitted to decrypt the message.

5. (original) The method of claim 4, wherein the access parameter is defined by the sender and is received at the management module from the sender.

6. (original) The method of claim 4, wherein the message code is received at the management module from the sender.

7. (original) The method of claim 4, wherein the access parameter is a default value known to the management module.

8. (original) The method of claim 4, wherein the message code is defined by the management module and transmitted to the sender for inclusion with the secure message.

9. (currently amended) ~~The method of claim 1,~~ A method for communicating between a sender and a receiver over a computer network, comprising the steps of:

defining a plurality of parameters for a secure message, at least one of the plurality of parameters accessible to a management module for controlling receiver access to a decryption key;

sending the secure message from the sender to the receiver over a network;

receiving the secure message at the receiver;

sending a request from the receiver to a management module for the decryption key;

processing the request at the management module to determine whether the receiver is permitted to decrypt the message based on said at least one of the plurality of parameters;

when not permitted, sending a denial message to the receiver;

when permitted, sending the decryption key to the receiver; and

when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, deleting the decryption key and the source-formatted decrypted message;

in which the step of processing the request at the management module to determine whether the receiver is permitted to view the message comprises: maintaining a count of a number of times that the decryption key has been sent to the ~~receiver; and~~ receiver, testing said at least one of the plurality of parameters accessible to the management module to determine whether the count exceeds a maximum number of times to send the decryption key to the receiver, and denying permission to decrypt the message when the count exceeds the maximum number.

10. (currently amended) The method of claim 1, ~~in which the step of processing the request at the management module to determine whether the receiver is permitted to view the message comprises:~~

~~testing said at least one of the plurality of parameters accessible to the management module to determine whether a permissible time for decrypting the secure message has expired.~~

wherein the source-formatted decrypted message is deleted after said reformatting without having been stored in permanent memory, wherein the prescribed format is a display format, and wherein the display formatted message is not retained after being displayed.

11. (original) The method of claim 1, in which the step of processing the request at the management module to determine whether the receiver is permitted to view the message comprises:

monitoring a contingent event specified in said at least one of the plurality of parameters accessible to the management module ; and

testing the contingent event to determine whether the decryption of the secure message by the receiver is permissible.

12. (original) The method of claim 1, wherein the prescribed format is a bit-mapped display format.

13. (currently amended) ~~The method of claim 1,~~ A method for communicating between a sender and a receiver over a computer network, comprising the steps of:

defining a plurality of parameters for a secure message, at least one of the plurality of parameters accessible to a management module for controlling receiver access to a decryption key;

sending the secure message from the sender to the receiver over a network;

receiving the secure message at the receiver;

sending a request from the receiver to a management module for the decryption key;

processing the request at the management module to determine whether the receiver is permitted to decrypt the message based on said at least one of the plurality of parameters;

when not permitted, sending a denial message to the receiver;

when permitted, sending the decryption key to the receiver; and

when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, deleting the decryption key and the source-formatted decrypted message;

wherein during the steps of decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message, interrupts are disabled at the receiver to prevent unauthorized access to the source-formatted decrypted message.

14. (currently amended) A method for communicating between a sender and a receiver over a computer network, comprising the steps of:

setting a send configuration parameter for a secure message;

routing the send configuration parameter to a management module;

sending the secure message from the sender to the receiver over a network;

receiving the secure message at the receiver;

sending a request from the receiver to the management module for a decryption key;

processing the request at the management module to determine whether the receiver is permitted to decrypt the message;

when not permitted, sending a denial message to the receiver;

when permitted, sending the decryption key to the receiver; and

when the decryption key is sent to the receiver, decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message without first storing the decryption key and source-formatted decrypted message in a permanent memory.

15. (currently amended) A system for securing communication between a sender and a receiver over a computer network, comprising:

a plurality of parameters pertaining to a secure message;

a management module which stores the plurality of parameters;

a communication pathway for carrying the secure message from the sender to the receiver over the network;

a communication pathway along which the receiver sends a request to the management module for a decryption key;

wherein the management module comprises means for processing the request to determine whether the receiver is permitted to decrypt the message, said processing means comprising means for testing at least one of said plurality of parameters;

means for sending a denial message to the receiver when the management module determines that decryption is not permitted;

means for sending the decryption key to the receiver when the management module determines that decryption is permitted;

processing means at the receiver for decrypting the message at the receiver into a source format, reformatting the decrypted message into a prescribed format, and deleting the decryption key and the source-formatted decrypted message without first storing the decryption key and source-formatted decrypted message in a permanent memory.

16. (original) The system of claim 15, wherein the plurality of parameters comprises: a maximum number of times that the secure message is permitted to be decrypted.

17. (original) The system of claim 15, wherein the plurality of parameters comprises: an expiration time after which the secure message is not permitted to be decrypted.

18. (original) The system of claim 15, wherein the plurality of parameters comprises: a parameter for determining a permissible time period during which the secure message is permitted to be decrypted.

19. (original) The system of claim 15, wherein the plurality of parameters comprises: a parameter which specifies a contingent event, wherein one of either the occurrence or nonoccurrence of said contingent event is testable to determine whether the secure message is permitted to be decrypted.

20. (original) The system of claim 15, wherein the management module resides with the sender.

21. (original) The system of claim 15, wherein the prescribed format is a bit-mapped display format.

22. (currently amended) The system of claim 15, comprising means for disabling interrupts at the receiver to prevent unauthorized access to the source-formatted decrypted message, while the processing means decrypts the message into the source format, reformats the decrypted message into the prescribed format, and deletes the decryption key and the source-formatted decrypted message.

23. (original) The system of claim 15, wherein the management module resides at a server computer in the network.

24. (not entered)

25. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the sender defines the message code and sends the message code to the management module.

26. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the sender defines the encryption key and sends the encryption key to the management module, the decryption key corresponding to the encryption key.

27. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the sender defines the access parameter and sends the access parameter to the management module.

28. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the management module defines the message code and sends the message code to the sender for inclusion with the secure message.

29. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the management module defines the encryption key and sends the encryption key to the sender, the decryption key corresponding to the encryption key.

30. (original) The system of claim 23, wherein the plurality of parameters comprises:

a message code, an encryption key and an access parameter, and wherein the access parameter is a default value known to the management module for use in processing the request.